IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNT "Allen Brookins," ACCOUNT IDENTIFIER NUMBER 100088817176829, THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	**MJ-23-** 138 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Wessel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector assigned to the United States Postal Inspection Service's ("USPIS") Mobile, Alabama Domicile. In this capacity, I am responsible for investigating criminal activity related to the United States Postal Service in the entire state of Mississippi and the

Southern District of Alabama. I have been a Postal Inspector since April 2021. Prior to becoming a Postal Inspector, I was employed as a Special Agent with the United States Naval Criminal Investigative Service since September 2015. I have received training at the Federal Law Enforcement Training Center in criminal investigations and financial crimes. I have a certificate in Forensic Accounting from Georgetown University and have been a Certified Fraud Examiner since 2012. In the course of my training and experience, I have worked on numerous investigations involving fraud. Pursuant to my duties as a Postal Inspector, I have gained experience in investigations of bank fraud pertaining to the theft, alteration, and counterfeiting of checks stolen from the U.S. mail. I have participated in search and seizure operations dealing with these types of criminal offenses. I have written, served, and reviewed the contents of the contents of multiple accounts operated on Meta platforms (including but not limited to Facebook) after obtaining the contents via search warrants related to altered and counterfeit checks.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. All dates, times, amounts, and locations referenced in my affidavit are approximations.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), and 1028A (aggravated identity theft) have been committed by **Allen Russel Brookins** ("**Brookins**") and others, both known and unknown. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated."

PROBABLE CAUSE

The Scheme

6. Since May 2023, I have been investigating numerous individuals, including but not limited to **Brookins**, for a counterfeit check-cashing scheme ("the scheme") involving the use of counterfeit identity documents to use the accounts of identity theft victims to cash fictitious checks at bank branches across multiple states, including within the Southern District of Alabama. The suspected participants are all connected to the Fort Lauderdale, Florida area and appear to operate with a modus operandi similar to a fraud scheme referred to as the "Felony Lane Gang." The Felony Lane Gang scheme often involves persons from the Fort Lauderdale, Florida area who travel the country committing various financial frauds involving identity theft, credit card fraud, and check-cashing schemes, and has been ongoing since at least 2015. These schemes often involve the use of rental vehicles to quickly move from jurisdiction to jurisdiction, frustrating local law enforcement's efforts to investigate and stop the unlawful activity.

7. On May 3, 2023, I called Victim 1, a businessman in Mississippi.[1] Victim 1 had contacted the USPIS to complain about personal and business checks of his that had been stolen after they were placed in the U.S. mail. Victim 1 stated to me that after his personal check was stolen, someone had used his identity to cash a stolen check using his bank account. Victim 1 stated that he had made a complaint to the Pearl, Mississippi Police Department ("PPD") and that he had been advised that PPD had identified a suspect in the investigation.

8. On May 3, 2023, I spoke to a PPD Detective (the "Detective") who shared his case file with me. This Detective advised me that on April 30, 2023, he went to the Community Bank[2] branch located at 2441 Old Brandon Rd, Pearl, Mississippi 39208, to talk to a bank employee regarding a complaint about a counterfeit check that was cashed using Victim 1's account. The bank employee told the Detective that at 9:30 am on March 20, 2023, a black male walked in wearing a business suit. Victim 1 is a white male. The black male walked up to the teller window and wanted to cash a check made out to a "[redacted]" for $3,069.14. According to the teller, the man had already signed and put a social security number on the back of the check. The teller asked for the man's ID, which was later determined by the Detective to be a fake Mississippi driver's license. The bank employee believed the ID to be real and there was money in the account, so the bank employee cashed the check. The black male left the bank with the cash and walked across the street, getting into a vehicle. A couple days later, the bank was contacted by Victim 1, who

[1] To protect the identities of the victims, all victims will be referred to using male pronouns regardless of their actual gender.

[2] Community Bank is insured by the Federal Deposit Insurance Corporation ("FDIC"). *See* https://banks.data.fdic.gov/bankfind-suite/bankfind.

said his identity had been stolen and he did not cash a check in Pearl, Mississippi on March 20, 2023. I interviewed the owner of the company against which the counterfeit check was written, who advised me that neither he nor his company issued the check and that his company had no such account at the bank whose routing number was affixed to the check.

9. The Detective compared bank surveillance images of the black man who presented the above-referenced fake Mississippi driver's license and cashed the above-referenced check to images posted on a Facebook account titled "**Allen Brookins**," located at URL https://www.facebook.com/profile.php?id=100088817176829, assigned account identifier number 100088817176829, which is the subject of this warrant application. The images on the Facebook page appeared to show the same person who had cashed the check wearing the same or a similar tie as the one worn by the black man who presented to fake Mississippi driver's license and cashed the check (*see* Figure 1 below).

Fig. 1 (Community Bank March 20, 2023, surveillance image on the left; image from **Brookins's** Facebook on the right).

10. The Detective determined that the individual in the photos is a real person—**Brookins**. The Detective obtained an image of **Brookins** via a law enforcement database. The

Detective requested that the Mississippi Fusion Center produce a photo line-up that included a law enforcement database photograph of **Brookins**. On April 27, 2023, a PPD Detective who was unfamiliar with the case administered a recorded photo lineup using the lineup provided by the Mississippi Fusion Center to the bank teller who cashed the above-referenced fraudulent check. The bank teller picked out the photo of **Brookins** as the person who had cashed the counterfeit check (*see* Figure 2 below).

Fig. 2 (photo lineup with **Brookins's** image identified by the Community Bank teller).

11. The Detective also received an image of the car in which **Brookins** was suspected to have left the bank. The car appeared to be a light-colored van. The Detective used license plate reader data to determine which light-colored vans matching that vehicle's description were in the jurisdiction of Pearl, Mississippi on the day the counterfeit check was cashed. The Detective identified one of the vehicles as a gray Chrysler minivan bearing South Dakota license plate

number 1DR528. This vehicle is registered to EAN Holdings, the registration holding company for the entity commonly known as Enterprise Rent-A-Car ("Enterprise"). The Detective called the Enterprise law enforcement support line. A dispatcher for Enterprise advised the Detective that the vehicle had been rented by two individuals from March 6, 2023, to April 5, 2023. One of those individuals was Terrill Q. Alexander ("Alexander"). I re-contacted the Enterprise law enforcement support line, which provided me with Alexander's date of birth, address, and phone number. The information provided was that Alexander's date of birth is [redacted] 1977, his address is [redacted], Opa-locka, Florida 33054, and primary number is [redacted]4642. I have reviewed Alexander's Florida driver's license data and determined that this is Alexander's current address.

12. Through my investigation, I became aware of other financial institutions that had a black male wearing a full or partial suit that deposited counterfeit checks. Origin Bank and Trustmark National Bank[3] provided me with certified business records including check images and surveillance images demonstrating that **Brookins** had also defrauded their institutions on March 20, 2023, by cashing checks using the stolen identities of Victim 2 in Jackson, Mississippi and Victim 3 in Flowood, Mississippi, in the same manner that Victim 1's identity was used at Community Bank (*see* Figures 3 and 4 below). These checks were written off the same account as the check used at Community Bank and appeared to be printed and written in the same style.

[3] Origin Bank and Trustmark National Bank are both insured by the FDIC. *See* https://banks.data.fdic.gov/bankfind-suite/bankfind.

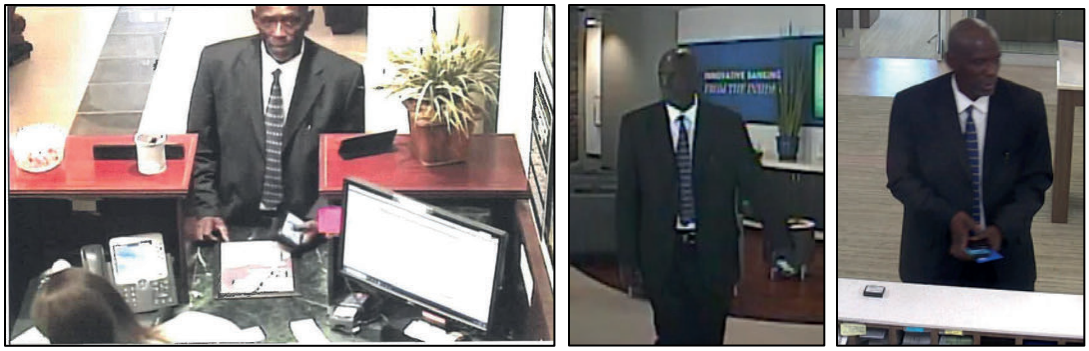


Fig. 3 (Community Bank March 20, 2023 surveillance image on the left; Origin Bank March 20, 2023 surveillance image in the center; Trustmark National Bank March 20, 2023 surveillance image on the right).

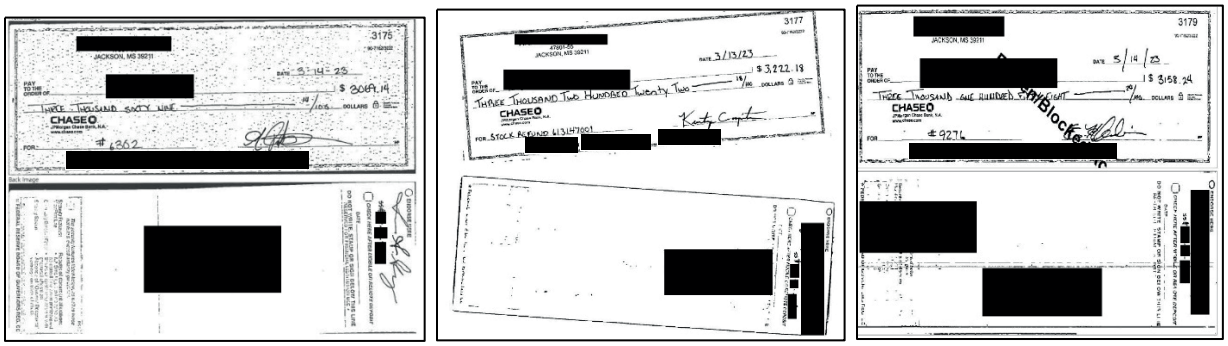


Fig. 4 (counterfeit checks passed on March 20, 2023, as referenced above).

13. Trustmark National Bank advised me that the same black male who appears to be **Brookins** had passed another counterfeit check at a branch in Mobile, Alabama on March 21, 2023, and provided me with certified records documenting the incident. The records show an image of what appears to be **Brookins** depositing a counterfeit check at the counter of a Trustmark National Bank branch in Mobile, Alabama using the identity of Victim 4 (*see* Figure 5 below). The check appears to be printed and written in a manner similar to the other checks described above (*see* Figure 6 below). Notes in the documentation show that the black male who appears to be **Brookins** produced a social security card and driver's license when the check was cashed in

Mobile, Alabama. Victim 4 was notified via a letter that was sent to him by Trustmark National Bank via the U.S. Mail that a check he had cashed had been reversed. Victim 4 complained to the bank and filled out an affidavit of identity theft. I have interviewed Victim 4, who confirmed to me that he was a victim of identity theft.

Fig. 5 (Trustmark National Bank March 21, 2023, surveillance image on the left; image from **Brookins's** Facebook on the right).

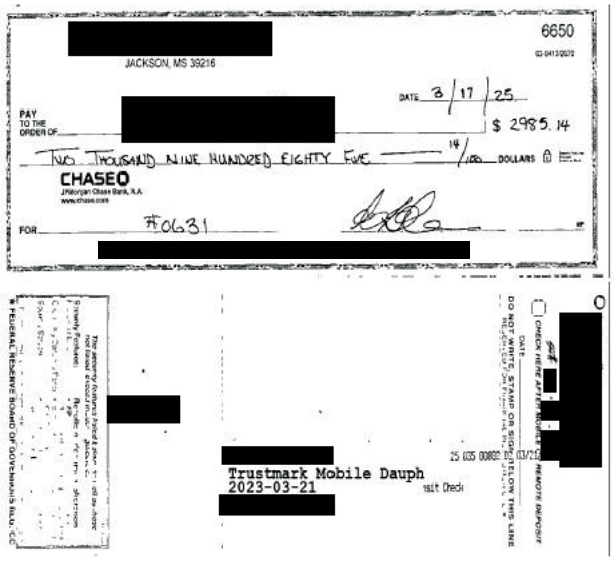


Fig. 6 (counterfeit check cashed using Victim 4's account in Mobile, Alabama).

14. I also communicated with City National Bank of West Virginia,[4] which advised me that at 9:56 am on April 12, 2023, a black male who appears to be **Brookins** cashed a counterfeit check using the City National Bank of West Virginia account of Victim 5 at a branch in Worthington, Ohio. City National Bank of West Virginia provided me with a surveillance image of a black male who appears to be **Brookins** conducting the transaction (*see* Figure 7 below), as well as an image of the counterfeit check that appears to have been written using the same printing and writing style as the counterfeit checks referenced above (*see* Figure 8 below).

Fig. 7 (City National Bank of West Virginia April 12, 2023 surveillance image).

[4] City National Bank of West Virginia is insured by the FDIC. *See* https://banks.data.fdic.gov/bankfind-suite/bankfind.

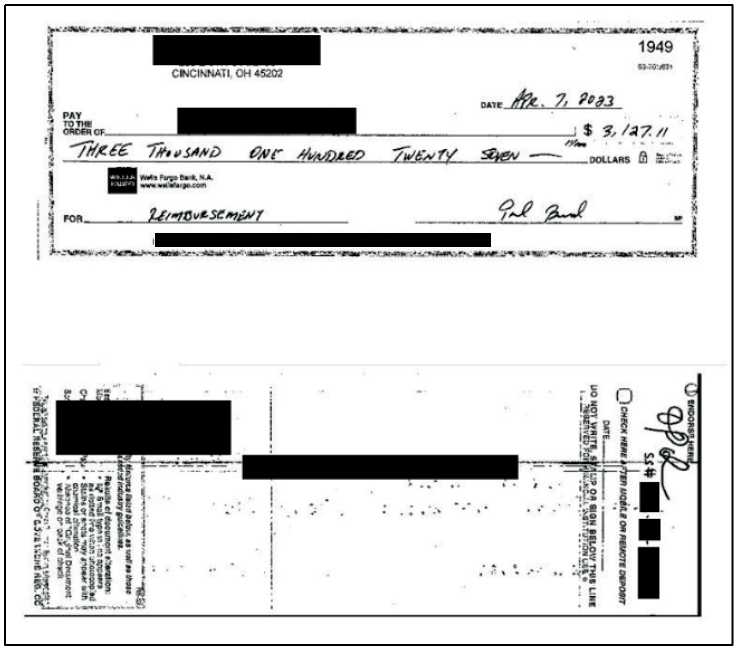


Fig. 8 (counterfeit check cashed using Victim 5's account at City National Bank of West Virginia).

15. I also communicated with The Northside Bank and Trust Company,[5] which advised me that at 12:51 pm on April 12, 2023, a black male who appears to be **Brookins** used a fake identification card to cash a counterfeit check using the identity and account of Victim 6 at a branch in Blue Ash, Ohio. The Northside Bank and Trust Company provided me with an affidavit from Victim 6 indicating that his endorsement was forged on the counterfeit check. The counterfeit check appears to be printed and written in the same manner as the counterfeit checks described above (*see* Figure 9 below). **Brookins** appears to be wearing the same clothes he was wearing in the surveillance image taken earlier in the same day that was provided to me by City National Bank of West Virginia (*see* Figure 10 below).

[5] The North Side Bank and Trust Company is insured by the FDIC. *See* https://banks.data.fdic.gov/bankfind-suite/bankfind.

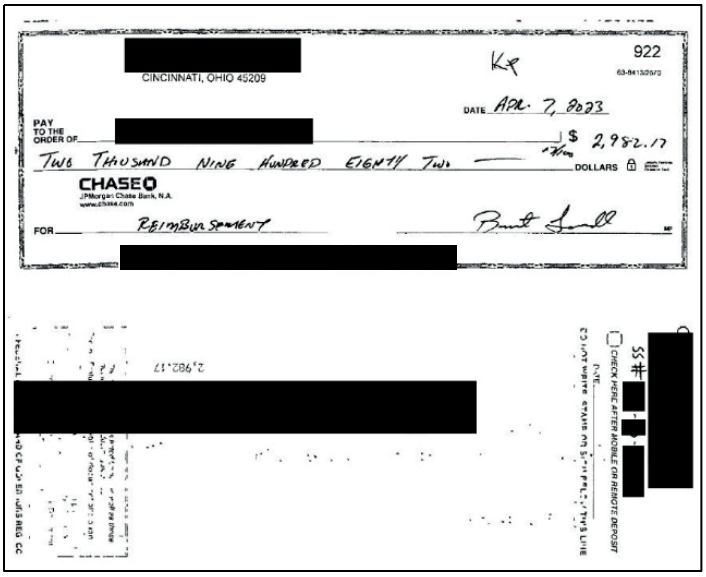


Fig. 9 (counterfeit check cashed using Victim 6's account at The Northside Bank and Trust Company).

Fig. 10 (The North Side Bank and Trust Company April 12, 2023 surveillance image).

16. At 1:15 pm on April 12, 2023, the Montgomery, Ohio Police Department ("MOPD") received a complaint from First Financial Bank[6] indicating that a black male was attempting to use a fake driver's license bearing Victim 7's name and personal identifying information to cash a suspicious check. MOPD officers arrived on scene a short time later. When they arrived, the black male fled on foot. The officers chased the black male and arrested him after a short foot chase. The black male was **Brookins**. MOPD officers verified via a visual review of the driver's license's features and a telephonic interview with Victim 7 that the driver's license was fake. During a search of **Brookins's** person incident to his arrest, MOPD officers discovered a check (*see* Figure 11 below). Officers called the company whose information was on the top left of the check. After speaking to an employee who denied the company had issued that check, the officers determined it was a counterfeit. **Brookins** was arrested wearing what appears to be the same clothes he was surveilled wearing at City National Bank of West Virginia and The North Side Bank and Trust Company earlier in the day (*see* Figure 12 below).

Fig. 11 (fake driver's license and counterfeit check recovered by MOPD officers who arrested **Brookins** on April 12, 2023).

[6] First Financial Bank is insured by the Federal Deposit Insurance Corporation. *See* https://banks.data.fdic.gov/bankfind-suite/bankfind.

Fig. 12 (image of **Brookins** in the MOPD holding cell in the clothes he was arrested in on April 12, 2023).

17. A short time after **Brookins** was arrested, MOPD was advised that Bethesda North Hospital security had located some checks and driver's licenses that they felt were suspicious. An MOPD officer arrived at their office and was informed that an unknown visitor had found a bank envelope in the parking lot and turned it into a security officer, who then delivered it to a security supervisor. Inside the envelope were driver's licenses, credit cards, checks, and post-it notes about banking information for various persons. Each bundle had a different name associated with it but had the same photo of **Brookins** as the driver's license bearing Victim 7's identity. Each bundle also had the name of a bank, the social security number of the owner, and additional names of various victims' accounts. Among those documents were a fake driver's license and credit card in the name of Victim 6 and an empty bank cash envelope from City National Bank of West Virginia's branch in Worthington, Ohio (*see* Figure 13 below).

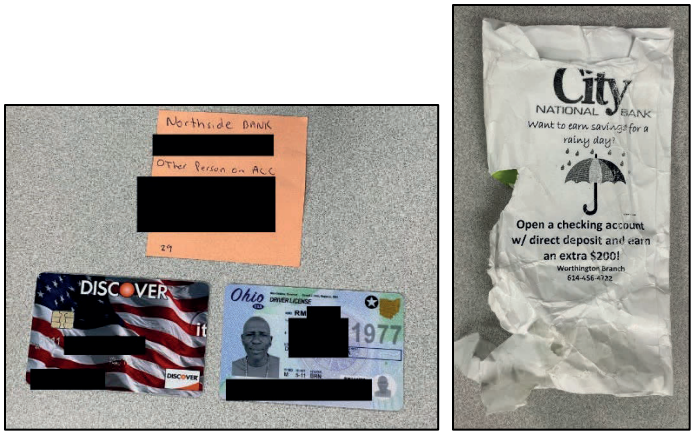
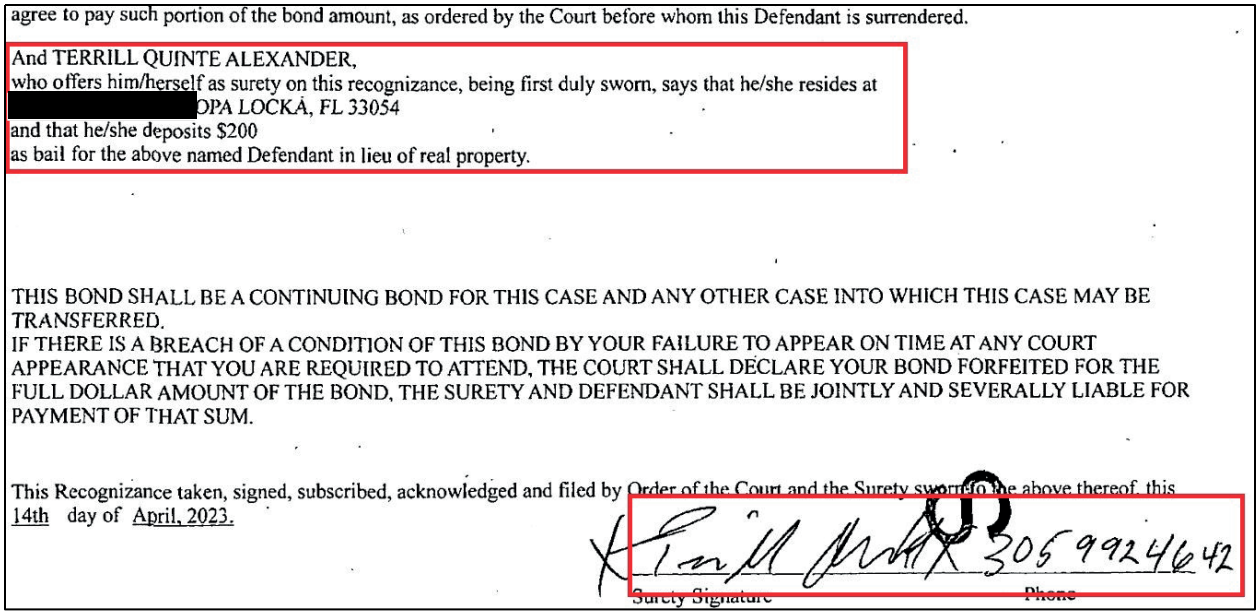


Fig. 13 (fake driver's license, fake credit card, and victim information for Victim 6 on the left; cash envelope for City National Bank of West Virginia's Worthington, Ohio branch on the right).

18. MOPD charged **Brookins** with various offenses related to his alleged attempt to cash a check using Victim 7's identity. **Brookins** was bonded out on April 14, 2023. The prosecutor for the case provided me with the charging documents and bond paperwork. The bond paperwork shows that **Brookins** was bonded out by Alexander. On the bond paperwork, Alexander's address and phone number are the same as the address and phone number that Alexander used to rent the car from Enterprise that was observed in the vicinity of the Pearl, Mississippi check-cashing incident as described above in paragraph 11 (*see* Figure 14 below).



agree to pay such portion of the bond amount, as ordered by the Court before whom this Defendant is surrendered.

And TERRILL QUINTE ALEXANDER,
who offers him/herself as surety on this recognizance, being first duly sworn, says that he/she resides at
[redacted]OPA LOCKA, FL 33054
and that he/she deposits $200
as bail for the above named Defendant in lieu of real property.

THIS BOND SHALL BE A CONTINUING BOND FOR THIS CASE AND ANY OTHER CASE INTO WHICH THIS CASE MAY BE TRANSFERRED.
IF THERE IS A BREACH OF A CONDITION OF THIS BOND BY YOUR FAILURE TO APPEAR ON TIME AT ANY COURT APPEARANCE THAT YOU ARE REQUIRED TO ATTEND, THE COURT SHALL DECLARE YOUR BOND FORFEITED FOR THE FULL DOLLAR AMOUNT OF THE BOND, THE SURETY AND DEFENDANT SHALL BE JOINTLY AND SEVERALLY LIABLE FOR PAYMENT OF THAT SUM.

This Recognizance taken, signed, subscribed, acknowledged and filed by Order of the Court and the Surety sworn to the above thereof, this 14th day of April, 2023.

305 992 4642

Surety Signature Phone

Fig. 14 (**Brookins's** bond documentation showing Alexander information).

19. The state prosecutor for this case advised me that **Brookins** did not appear for his first scheduled court appearance after he was bonded out. I have been advised by a Detective from the Lawrence, Kansas Police Department ("LPD") that **Brookins** was observed on surveillance video repeating this scheme in two cities in Kansas on April 28, 2023, and April 29, 2023. I have reviewed surveillance images provided by LPD, and they appear to be of **Brookins**. I have not yet received copies of the full bank documentation pertaining to these incidents, but what I have observed and from what the LPD advised me, the checks appear to be printed and written in the same manner as the counterfeit checks noted above and were passed in a similar manner to the counterfeit checks noted above.

20. I reviewed files provided by LPD regarding the April 28, 2023, incident. During this incident, **Brookins** was observed on surveillance camera using a driver's license with Victim 8's identity to cash a check. External bank surveillance video appears to show a dark-colored, four-door SUV pull into the far end of the bank's shared parking lot just off frame. Shortly

after, **Brookins** enters the frame and walks across the parking lot into the bank. After leaving the bank, **Brookins** exits the frame in the direction of where the SUV pulled in. The SUV then exits the parking lot and drives away. The SUV is visible from a side profile. An LPD Detective conducted a license plate reader search for similar vehicles in the area, and identified two possible matches. One of the matches was a Ford Edge bearing Oklahoma License plate number MFG414. This vehicle was identified two miles from the bank where Victim 8's identity was used by **Brookins** to cash a check two hours after the check was cashed. I conducted a database check on the vehicle, and discovered that it was owned by Enterprise. I called the Enterprise law enforcement support line. A dispatcher for Enterprise advised me that on April 28, 2023, that vehicle was rented by Alexander.

21. Alexander's Florida driver's License bears the address [redacted], Opa-locka, Florida 33054.[7] Having identified Alexander as a person in proximity to these incidents, I conducted database searches to identify other law enforcement files pertaining to Alexander. The chronologically first file that I was able to identify regarding Alexander and allegations of fraud was a December 11, 2017, report by the Apple Valley, Minnesota Police Department ("AVPD"). According to the report, on December 11, 2017, two officers were dispatched to a Bank of America regarding a report of a female attempting to cash a forged check with a fake identification. The bank advised the officers that the female had been at the bank the week prior with another fake identification. The officers stopped the female, who was in possession of an identification card bearing another person's name. She advised the officers that

[7] This is the same address Alexander used to rent both rental vehicles noted above.

her husband and two black males had dropped her off in a maroon station wagon with a roof rack to cash a counterfeit check. One of the officers recognized the car as one whose license plate he had run earlier. A short time later, the officer heard radio traffic that a neighboring jurisdiction had pulled over that car. The officer went to the vehicle stop and observed that the driver was Alexander (*see* Figure 15 below). During an interview, one of the other passengers of the vehicle admitted to law enforcement that he and his wife had traveled to Minnesota with Alexander to commit check fraud and make some money. The investigative report indicates that the female and her husband were from the Opa-locka, Florida area.

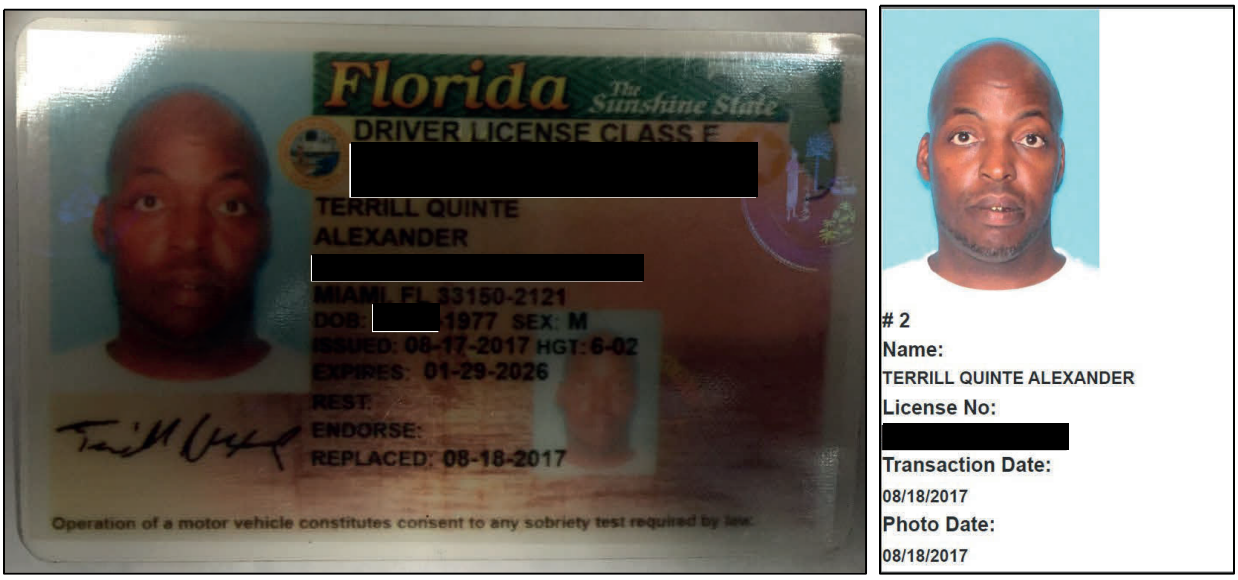


Fig. 15 (Alexander's driver's license as photographed by AVPD in 2019; corresponding Florida driver's license information for Alexander).

22. I was also able to identify a 2019 police report from the Roanoke County, Virginia Police Department documenting a counterfeit check-cashing scheme in which the check casher was arrested noted that the check casher was associated to a rental car that had been rented by Alexander. The check casher was from Florida near Fort Lauderdale, Florida. She was found guilty

of a state offense related to attempting to pass the counterfeit check, released, and placed on probation where she was allowed to move to Ohio. Her most recent address I could identify is in Ohio near where Brookins was arrested for attempting to cash a check using Victim 7's identity.

23. In May 2023, I made contact with a Kentucky State Trooper assigned to Kentucky State Police ("KSP") Campbellsburg Post 5. The Trooper advised me that on March 1, 2023, the Trooper had arrested Alexander. The Trooper shared his police report and Alexander's citation with me. According to the documents, on March 1, 2023, the Trooper observed a white Toyota passenger car traveling at a high rate of speed. The Trooper pulled over the vehicle, which was driven by Alexander and had two passengers ("Passenger 1" and "Passenger 2"). The Trooper smelled marijuana. Passenger 1 admitted he had a bag of marijuana in the waistband of his pants and surrendered the bag to the Trooper. The Trooper then ordered all occupants out of the vehicle and requested another Trooper's assistance.

24. The Trooper began searching the immediate area of the vehicle's occupants. The occupants stated they were traveling from Florida and had all their luggage in the rear of the vehicle. The Trooper then began searching each bag and located a smaller gray/black bag. Inside the bag, the Trooper located some clothing items and underneath the clothing was clear plastic baggie of suspected cocaine, an unknown amount of U.S. currency in cash, multiple identification cards with the same picture but different names and addresses, multiple forged checks, several blank checks, and multiple paper clippings with personal information written on them. Passenger 1

admitted ownership of the suspected cocaine,[8] but none of the occupants claimed ownership of the other documents. During the vehicle search, all the occupants stood near the front of the vehicle. While standing there, Alexander attempted to throw two pieces of crumbled up paper into the tree line. The second Trooper observed this and handcuffed Alexander. The primary Trooper then walked to where the items were thrown and identified them as banking envelopes.

25. Upon further review of the items, the Troopers discovered that each ID had a corresponding Discover card, forged checks, blank checks, and the actual owners' banking information and social security numbers. After running each driver's license number through dispatch, they advised that several of them came back to real individuals. Alexander and the vehicle's other occupants were then placed under arrest. While searching Alexander incident to his arrest, the primary Trooper located a large amount of U.S. currency (*see* Figure 16 below).

Fig. 16 (counterfeit documents recovered by KSP on the left; cash recovered by KSP on the right).

[8] Laboratory examination later determined the substance to be a different synthetic drug banned under Kentucky law.

26. Of significance, the checks associated to **Brookins** in this investigation and various notes recovered with victim personal information contained victim social security numbers written in the format "ss# xxx-xx-xxxx." The victim personal information recovered by the Troopers on the above-referenced traffic stop were written in the same manner, along with similar Discover credit cards bearing the names on the counterfeit driver's licenses (*see* Figure 17 below). Given my knowledge, training, experience, and review of the various documents pertaining to this investigation, I believe there is probable cause that the conspirators in this matter produce fake credit cards with sixteen digit numbers and the names of the various identity theft victims as secondary forms of identification if challenged by a bank teller.

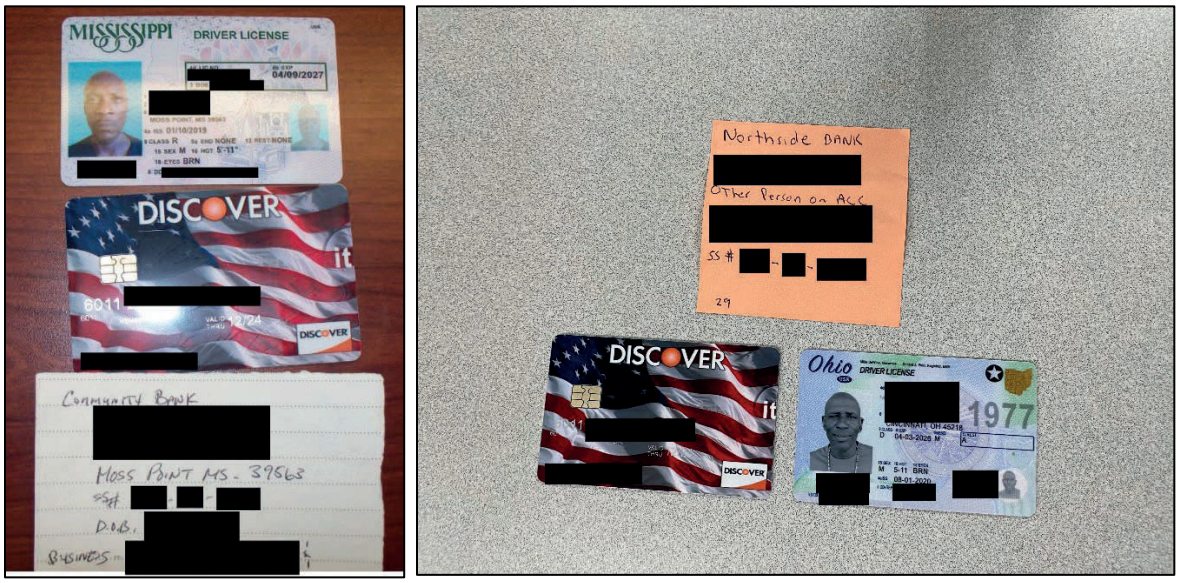


Fig. 17 (documents pertaining to a victim recovered by KSP on the left; items with Victim 7's name on them recovered by MOPD on the right).

The "Allen Brookins" Facebook Page

27. As noted above, **Brookins** was partially identified by comparing bank surveillance images against pictures of a black male on a Facebook account titled "**Allen Brookins**," located

at URL https://www.facebook.com/profile.php?id=100088817176829, assigned account identifier number 100088817176829. I have reviewed this Facebook page's public information. Based on my knowledge, training, and experience, this Facebook page operates in a manner consistent with a Facebook page operated by an individual, and includes photos posted of **Brookins** with other persons, **Brookins** alone, and "selfie" style photographs of **Brookins**. The page also has interactions with other accounts that are publicly visible, including shared posts from other pages and other pages "liking" or otherwise reacting[9] to posts made by this page. I observed that the page made various posts of images, text, and videos from December 23, 2022, through April 22, 2023. I obtained records from Meta indicating that this account was registered on December 23, 2022. The records state the email address used to register the account was [redacted]@gmail.com. The records also that the Facebook page "Allen Brookins" has the account identifier number "100088817176829," which is a unique account identifier to this page that will remain the same regardless of if the vanity name ("**Allen Brookins**") is changed, similar to how a person's social security number typically stays the same even if their legal name changes. Based on my knowledge, training, and experience, I know this identifier to be a unique number assigned to the Facebook page that will stay with it regardless of how the page's display name may change.

28. Based on my knowledge, training, and experience, I believe that that Meta retains information pertaining to Facebook accounts that, if seized as evidence and reviewed by law enforcement, would provide more information on **Brookins's** involvement in the scheme, identify

[9] Facebook users can choose to like, laugh, love, or otherwise react to posts made by other users.

additional victimized persons and financial institutions, and identify potential co-conspirators. For example, I know that Meta retains Internet Protocol ("IP") address information documenting the location from which accounts have been logged in. This information can assist with identifying locations **Brookins** stopped in for long periods of time between the first and last known instances of bank fraud, potentially identifying additional jurisdictions in which **Brookins** committed acts of fraud where he remains an unknown suspect. I have also observed that the "**Allen Brookins**" Facebook page has commented back and forth with other pages in the comments section of photographs posted to the "**Allen Brookins**" Facebook page. This indicates to me that **Brookins** is familiar with Facebook's various messaging features, and likely communicated with others via Facebook's private messaging feature. Given that it appears **Brookins** has been traveling across the country to commit this scheme, I believe there is probable cause that he discussed his travels, locations, and other details relevant to this investigation using Facebook's private messaging feature. I believe this is highly likely given that on April 1, 2023, the Facebook page "**Allen Brookins**" posted a photo of what appears to be **Brookins** in the same suit he was surveilled defrauding Trustmark National Bank in on March 21, 2023. The Facebook page "**Allen Brookins**" also posted an image of **Brookins** in what appears to be the same suit on December 23, 2022 (*see* Figure 18 below).

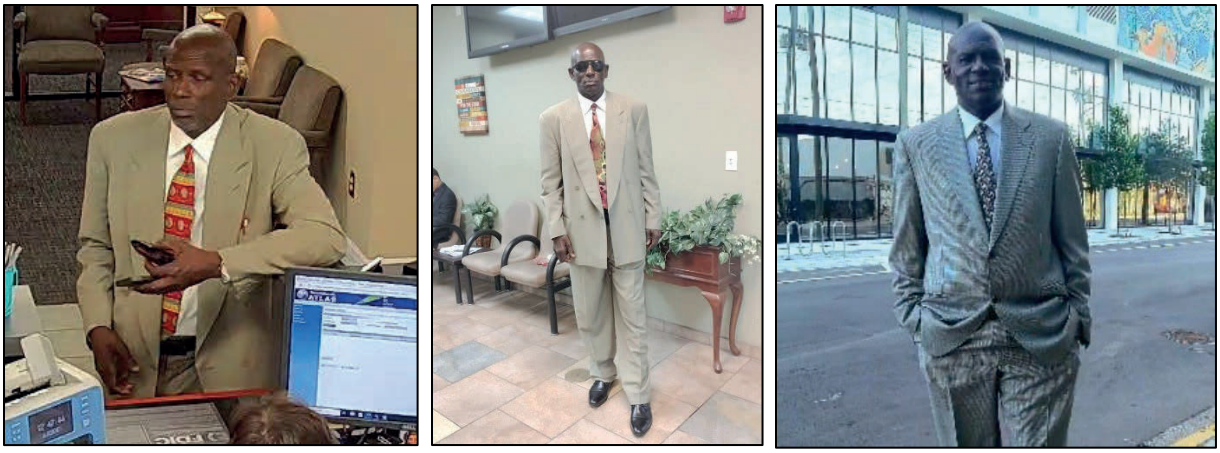


Fig. 18 (Trustmark National Bank March 21, 2023 surveillance image on the left; Facebook image posted on April 1, 2023 in the center; Facebook image posted on December 23, 2022 on the right).

29. Given the above, I believe there is probable cause to believe that the Facebook account titled "**Allen Brookins**," located at URL https://www.facebook.com/profile.php?id=100088817176829, assigned account identifier number 100088817176829, contains evidence of violations of 18 U.S.C. §§ 1349 (fraud conspiracy), 1344 (bank fraud), 513(a) (possession of counterfeited or forged securities), and 1028A (aggravated identity theft).

BACKGROUND CONCERNING FACEBOOK[10]

30. Facebook is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically,

[10] The information in this section is based on information published by Meta on its Facebook website, including, but not limited to, the following webpages: "Privacy Policy," https://www.facebook.com/privacy/policy/; "Information for Law Enforcement," https://www.facebook.com/help/494561080557017; and "Help Center," https://www.facebook.com/help.

Facebook is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Facebook accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Facebook users and the general public.

31. Meta collects basic contact and personal identifying information from users during the Facebook registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

32. Meta also collects and retains information about how each user accesses and uses Facebook. This includes information about the IP addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

33. Each Facebook account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose. Facebook users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

34. Facebook users can also connect their Facebook and Facebook accounts to utilize certain cross-platform features, and multiple Facebook accounts can be connected to a single Facebook account. Facebook accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Facebook user can "tweet" an image uploaded to Facebook to a connected Twitter account or post it to a connected Facebook account,

or transfer an image from Facebook to a connected image printing service. Meta maintains records of changed Facebook usernames, associated Facebook accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

35. Facebook users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Facebook also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

36. Users have several ways to search for friends and associates to follow on Facebook, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Facebook users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Facebook users. Users can also manually search for friends or associates.

37. Each Facebook user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, employment, and other biographical details.

38. One of Facebook's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their

devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

39. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Facebook. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment). A Facebook post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

40. A Facebook "story" is similar to a post but can be viewed by other users for specific periods of time, often just 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. Other users can react to or comment on the story images/video.

41. Facebook allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Facebook upon completion unless the creator chooses to save it using a long-form video app.

42. Facebook Messenger, Facebook's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Facebook Messenger also enables users to video chat with each other directly or in groups.

43. Facebook offers services such as Facebook Marketplace and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Facebook platform as well as on Facebook and other associated websites and apps. Facebook collects and retains payment information, billing records, and transactional and other information when these services are utilized.

44. Facebook has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable from Facebook. Meta retains records of a user's search history.

45. Meta collects and retains location information relating to the use of a Facebook account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

46. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Facebook users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

47. In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

48. For each Facebook user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

49. In my training and experience, evidence of who was using Meta, Inc. platform based accounts and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

50. For example, the stored communications and files connected to a Facebook account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

51. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique

hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

52. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

53. Other information connected to the use of Facebook may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, stored communications, contact lists, photos, and videos can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

54. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Facebook. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

55. Based on the forgoing, I request that the Court issue the proposed search warrant.

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Daniel Wessel
Postal Inspector
U.S. Postal Inspection Service

THE ABOVE AGENT HAS ATTESTED TO THIS AFFIDAVIT PURSUANT TO FED. R. CRIM. P. 4.1(b)(2)(B) THIS 6th DAY OF JUNE 2023.

P. Bradley Murray
Digitally signed by P. Bradley Murray
Date: 2023.06.06 14:40:16 -05'00'

P. BRADLEY MURRAY
UNITED STATES MAGISTRATE JUDGE

SEALED

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook account titled "**Allen Brookins**," located at URL https://www.facebook.com/profile.php?id=100088817176829, assigned account identifier number 100088817176829, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1601 Willow Road, Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Facebook usernames (past and current) and the date and time each username was active, all associated Facebook and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers **from December 23, 2022, to present**;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, **from December 23, 2022, to present**;

C. All content, records, and other information relating to communications sent from or received by the account **from December 23, 2022, to present**, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Facebook users **from December 23, 2022, to present**, including but not limited to:

1. Interactions by other Facebook or Facebook users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to

follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account **from December 23, 2022, to present**; and

F. All location information, including location history, login activity, information geotags, and related metadata **from December 23, 2022, to present**.

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1349, 1344, 513(a), and 1028A, those violations involving **Allen Russell Brookins**, and any coconspirators, and occurring on or after December 23, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. Evidence of the stealing of mail, the manufacturing of counterfeit checks, manufacture of counterfeit credit cards, the depositing of counterfeit checks, the solicitation of individuals to participate in counterfeit check cashing, preparatory steps taken in furtherance of the scheme, money laundering, wire fraud, bank fraud, and aggravated identity theft;

B. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

C. Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and

D. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).